## HOME AND ROAMING PROVISIONING METHOD FOR MOBILE TERMINALS

## BACKGROUND OF THE INVENTION

### Field of the invention

The present invention relates to setting up connections to a data network for terminals, in particular mobile terminals, and more particularly to the provision of data needed to set up a connection.

### Description of the prior art

It is well known in the art that setting up connections across a packet-switched data network such as the Internet involves allocating an address to the data network. For most uses address allocation is dynamic and effected by a service provider to which the user subscribes. The expression "primary provision" or "primary data provision" refers to the step of supplying a user with data for establishing a first connection to a service provider. That data includes all the parameters of all the layers needed for the connection to the service provider, for example the telephone number, the transmission medium employed, a user login name, a password, etc. In the case of a connection to a service provider using a computer, the primary provision is often effected by supplying the user with a CD-ROM containing the provisioning data, with a temporary address. It is also known in the art to provide the primary provisioning data by mail; the data is then copied by the user when prompted to do so, using appropriate software.

Mobile terminals are now appearing which have an Internet connection terminal function in addition to a telephone network terminal function. For terminals of this kind the telephone network provides the access network to the data network. Solutions to the problem of primary provisioning for such terminals have been proposed. Patent applications filed on the same day as the present application, whose titles in translation are "Method of validating data in a terminal" and "Method of validating the primary provisioning of a terminal" provide advantageous solutions for provisioning mobile terminals. The provisioning data is then stored in a physical location or in a logical file of the terminal and is updated if necessary during the next provisioning.

It is also known in the art to enable mobile terminals to use different public land mobile networks (PLMN). A mobile terminal or a user terminal is usually associated with a given public land mobile network or home access network, which is the access network to which they subscribe. The facility to connect to other public networks can also be provided. The term "roaming" refers to a change of network on

2

moving from one access network to another.

A new problem encountered with mobile terminals which can connect to a data network is that of provisioning in the case of a change of access network. If the access network is changed, it is necessary to update the provisioning data in the terminal in order to be able to continue to access the services of the data network. On returning to the home access network, further provisioning is then required to reload the provisioning data for the home network.

This problem encountered on "roaming" between access networks also applies to "roaming" between users, i.e. if the same terminal is used by more than one user, for example with different subscriber identification module (SIM) cards. The expression "plastic roaming" is used to refer to a change of user by changing SIM card.

The invention provides a solution to the above new problems. It enables a change of user or access network without losing the provisioning data. Returning to the home access network or another change of user is possible without it being necessary to carry out further provisioning.

## SUMMARY OF THE INVENTION

To be more precise, the invention proposes a telecommunication terminal for accessing a data network via an access network using a set of provisioning data, the terminal having means for storing a current set of provisioning data and means for storing at least one set of protected provisioning data that cannot be updated without the intervention of the terminal user.

The invention also proposes a method of updating provisioning data in a telecommunications terminal for accessing a data network via an access network and an access provider, the method including the steps of:

- backing up provisioning data for an access network, an access provider or a user; and

- protecting the backed up provisioning data to prevent it being updated without the intervention of the user, an access network operator or the access provider.

## BRIEF DESCRIPTION OF THE DRAWINGS

Other features and advantages of the invention will become apparent on reading the following description of embodiments of the invention, which description is given by way of example and with reference to the single figure, which is a flowchart of a method in accordance with the invention.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

To avoid updating the provisioning data if the access network or user is changed, the invention proposes to provide a terminal with protected provisioning data storage means. The provisioning data is not updated automatically if the user changes, the access network changes or the provisioning is updated, but only if the user intervenes. The invention therefore enables the provisioning data to be used again on returning to the home access network, or if the user changes, without further provisioning. The current provisioning data is then either a copy of the protected data or the protected data itself.

As indicated above, in prior art terminals the provisioning data is stored in a logical file or in a physical location in the terminal and is updated on the occasion of each new provisioning. Such updating can occur if the access network is changed and the user of the terminal carries out a provisioning in the new network; it can also occur if the user is changed and the new user carries out a new provisioning. It can also be a question of a provisioning for a new access to the Internet via a new service provider.

The invention proposes to enable not only storing the current provisioning data in a terminal but also storing protected positioning data in the terminal, which data is updated only on the intervention of the user.

In a first embodiment the protected provisioning data is provisioning data corresponding to a particular access network referred to as the home access network. The home access network is the usual access network of the user of the terminal. If the access network is changed temporarily, the user loads new provisioning data, which is stored in the file for storing the current provisioning data. The user can then access data services using the current provisioning data. On returning to the home access network, the provisioning data contained in the protected provisioning data storage means can be copied into the means for storing the current provisioning data; it is then possible to access the data network without having to carry out further provisioning.

In a second embodiment the protected provisioning data is provisioning data corresponding to a given user of a particular access network. It is then possible, for the same access network, to change the access network user without having to carry out further provisioning.

In these first two embodiments the provisioning data can be stored in a medium dedicated to the access network or to the user in the access network. That

4

medium is typically an SIM card in the case of a GSM telephone access network. The home access network is the home PLMN and the user is identified by their international mobile subscriber identity (IMSI).

In a third embodiment the protected provisioning data is data corresponding to more than one possible access to the data network. This is typically the case with a plurality of data network access providers. The user can then store protected provisioning data corresponding to a usual access to the data network. The user can then carry out provisioning for another access to the data network, for example via another access provider; the user can revert to the old access provider by copying the provisioning data contained in the protected provisioning data storage means.

In a fourth embodiment the protected provisioning data is provisioning data corresponding to a given user for a particular access provider. It is then possible, for the same access provider, to change the user identity without having to carry out further provisioning.

In the third and fourth embodiments the provisioning data can be stored in a medium dedicated to the access provider or service provider, and typically in a wireless application protocol (WAP) identification module (WIM).

Fifth and sixth embodiments of the invention propose to store protected provisioning data for a plurality of content providers or for a plurality of users at the content providers.

In all embodiments there can be provision for storing a plurality of sets of provisioning data corresponding to a plurality of access networks, to a plurality of access network users, to a plurality of data network accesses or access providers, to a plurality of users identified by a data network access provider, to a plurality of content providers, or to a plurality of users for a content provider. It is then advantageous to store for each set of provisioning data indications of the access network, the access network user, the access provider, the access provider user, the content provider or the corresponding user.

From the hardware point of view, the protected provisioning data storage means can be in the terminal itself, in a medium dedicated to the access or content provider, or in a medium dedicated to the access network or the access network user. The number of sets of provisioning data on each medium depends on the size of the medium.

The flowchart in the figure shows one embodiment of a method in accordance with the invention in the case where the mobile terminal automatically

5

selects an appropriate set of provisioning data. In the figure, protected provisioning data storage means are provided:

- in a medium dedicated to an access provider - in the example a WIM card;

- in a medium dedicated to a type of access network and to a user - in the example an SIM card; and

- in the mobile terminal itself.

In each case identification data is stored for each set of protected provisioning data. The provisioning data used is managed by the mobile terminal in accordance with data stored in the WIM card or in the SIM card or in the terminal.

The steps of the flowchart shown in the figure can be executed when the terminal is turned on, when an SIM card is inserted or when a WIM card is inserted. When it is turned on, and in a manner that is known in the art, the terminal identifies a user and a usable telephone network (this is step 2 in the figure). The next step is step 4.

In step 4, the terminal determines if a WIM card is present. If so, the next step is step 6; if not, the next step is step 14.

In step 6, the terminal determines if the WIM card contains protected provisioning data for the user of the WIM card and the current access network. If so, the next step is step 8; if not, the next step is step 10.

In step 8, the provisioning data obtained is selected to enable access to the data network. The process terminates.

In the above steps, the selection of the user of the WIM card is implicit, in that the WIM card is dedicated to one user. It is nevertheless possible to verify the identity of the terminal user by prompting the user to enter at the terminal a personal identification number before enabling the user to use the provisioning data contained in the WIM card.

In step 10, the terminal determines if the WIM card contains files providing for a change of access network (roaming files). If so, the terminal verifies if those files contain provisioning data or if necessary requests provisioning data from the network. The provisioning data can then be stored in the WIM card roaming file and used as indicated in step 12, and the process terminates. If not, the next step is step 32.

The figure does not show the facility for prompting the user to store the provisioning data obtained in step 12 in the protected storage means; the data can be stored in the terminal and/or in the WIM card.

In step 14, it is known that there is no WIM card in the terminal. It is then

determined if there is an SIM card in the terminal. If so, the next step is step 16; if not, the next step is step 24.

In step 16, the terminal determines if the SIM card contains protected provisioning data corresponding to the user and to the telephone network that has been identified. If so, the next step is step 18; if not, the next step is step 20.

In step 18, the provisioning data obtained in the SIM card is selected to enable access to the data network. The process terminates.

In the above steps, the selection of the user of the SIM card is implicit in that the SIM card is dedicated to a user. As in the case of the WIM card, it is possible to verify the identity of the terminal user by prompting the user to enter at the terminal a personal identification number before enabling the user to use the provisioning data contained in the SIM card.

In step 20, the terminal determines if the SIM card, if it does not contain usable provisioning data, contains roaming files providing for a change of access network. If so, the terminal determines if the roaming file contains provisioning data or if necessary requests the corresponding provisioning data, stores it in the SIM card roaming file, and uses the corresponding data as indicated in step 22, and the process terminates. If not, the next step is step 24.

As for step 12, the figure does not show the facility to prompt the user to store the provisioning data obtained in step 22 in the protective storage means of the SIM card.

In step 24, it is known that there is no provisioning data stored in the WIM card or in the SIM card or available from roaming files. It is determined whether the terminal itself contains protected provisioning data corresponding to the user or the telephone network that has been identified. If so, the next step is step 26; if not, the next step is step 28.

In step 26, the provisioning data obtained in the terminal is selected to enable access to the data network. The process terminates.

In step 28, it is determined if the terminal, if it does not contain usable provisioning data, contains roaming files providing for a change of access network. If so, the terminal requests the corresponding provisioning data, stores it in its roaming file, and uses the corresponding data, as indicated in step 30, and the process terminates. If not, the next step is step 32.

As for steps 12 and 22, the figure does not show the facility for prompting the user to store the provisioning data obtained in step 30 in the protected storage

means of the terminal.

In step 32, it is known that there is no provisioning data either stored or available by means of the roaming files. The process terminates, and provisioning is required.

The process shown in the figure corresponds to an order of decreasing priority for provisioning data stored in the WIM card, in the SIM card or in the terminal. There is no facility for a change of user.

The data stored in the protected provisioning data storage means is preferably erased only on the intervention of the user, either by deleting the corresponding data or by means of an update, as indicated above with reference to steps 12, 22 and 26.

Of course, the invention is not limited to the preferred embodiments described above. It applies to access network types other than the GSM network. In particular, the priority order stated for the example shown in the figure can be changed, as can the place where provisioning data is stored or the type of identification proposed for the provisioning data.

More generally, the invention applies to all types of access network, for example a fixed telephone network, the GSM network or other access network formats. The terminal can therefore be not only a mobile terminal but also a fixed terminal in the case of an access network consisting of a fixed telephone network or another type of terminal for another type of network.

The only data network referred to in the examples is the Internet. The invention can be applied to other types of packet-switched network, for example a WAP network or an X.25 network such as the Transpac network, using a packet assembling/disassembling (PAD) protocol.

In the examples, the protected data cannot be updated or deleted without the intervention of the terminal user. It is also possible to enable modification or deletion of data only by an operator or by the service or content provider; conjoint intervention of the access network operator, the access or content provider and/or the user is also possible.

In all the examples the protected data storage means are "in" the terminal. This means that the protected data is stored either in the terminal itself or in a medium which is integrated with the terminal in normal use, for example an SIM card or a WIM card.